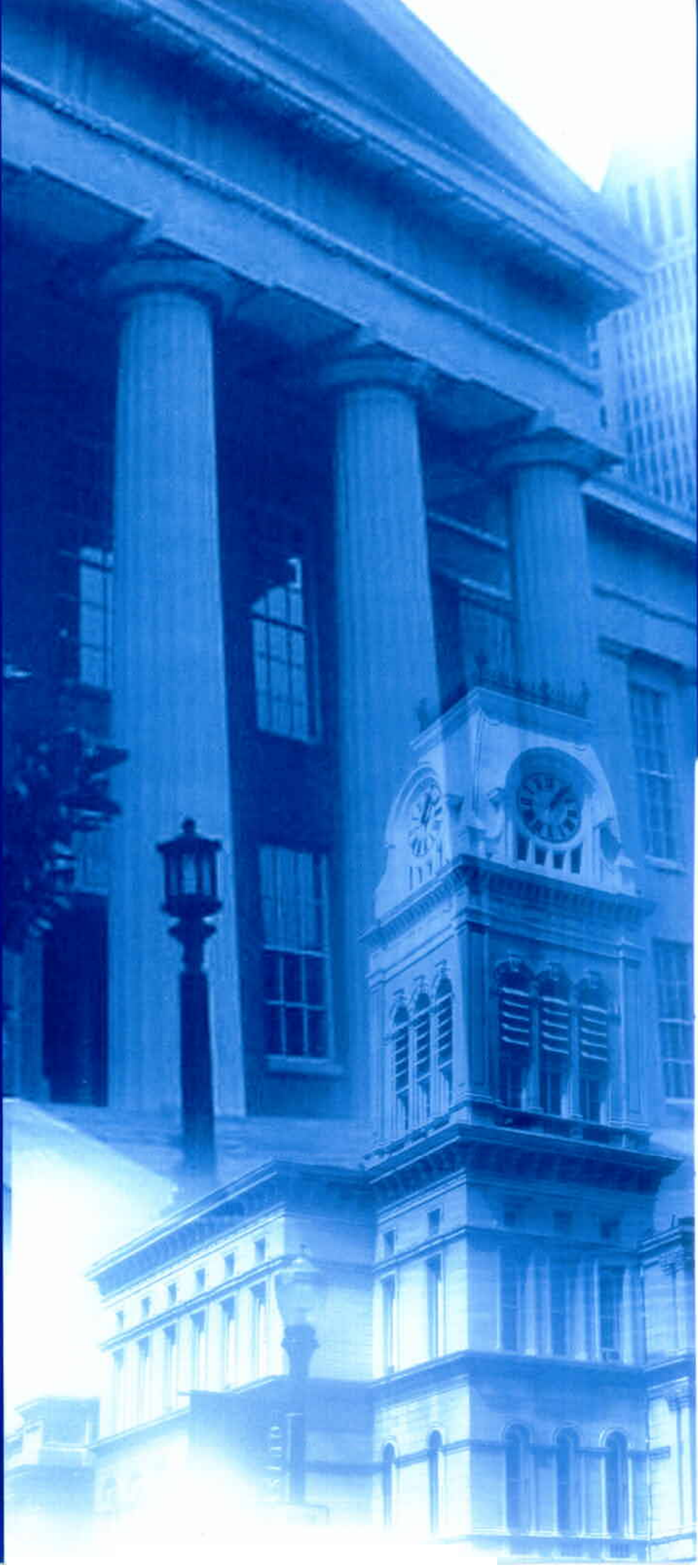
Office of Internal Audit

LOUISVILLE · JEFFERSON COUNTY
17 78
METRO

Jerry E. Abramson
Mayor

26 Member
Metro Council



The Office of Internal Audit provides independent, objective assurance and consulting services that adds value to and improves Louisville Metro Government.

Audit Report

Youth Center

IS General Controls

April 2004

Office of Internal Audit

Youth Center

IS General Controls

Table of Contents

JERRY E. ABRAMSON
MAYOR

KELLY DOWNARD
PRESIDENT, METRO COUNCIL

LOUISVILLE, KENTUCKY

OFFICE OF INTERNAL AUDIT

MICHAEL S. NORMAN, CIA
CHIEF AUDIT EXECUTIVE

Transmittal Letter

April 19, 2004

The Honorable Jerry E. Abramson
Mayor of Louisville Metro
Louisville Metro Hall

Re: Audit of Youth Center's Information Systems General Controls

Scope and Opinion

We have examined the adequacy of the general controls for information systems used by the Youth Center. The purpose was to ensure assets are adequately safeguarded, data files and software are secured, technical and administrative support are adequate, and management support and awareness of the system function is adequate. The primary focus of the audit was those systems not under the direct support of Metro Department of Technology. In-depth technical system auditing was not performed.

As a part of our examination, we performed an evaluation of the internal control structure. Our examination was conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States and with the Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors.

The objective of internal control is to provide reasonable, but not absolute, assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safeguarding of assets

There are inherent limitations in any system of internal control. Errors may result from misunderstanding of instructions, mistakes of judgment, carelessness, or other personnel factors. Some controls may be circumvented by collusion. Similarly, management may circumvent control procedures by administrative oversight.

The general controls for the information systems used by the Youth Center were reviewed through interviews with key personnel. The interviews were structured using various IT audit best practices and guidelines. For example, a specific resource tool used was the CoBIT (Control Objectives for Information and related Technology) framework of internal control. The resource tools help to substantiate the opinion regarding Youth's understanding and management of risks associated with information and related information technology. The specific systems reviewed included the following:

- Home Incarceration System
- Juvenile Court Activity Tracking System (JCATS)
- Master Control Security System

The scope and methodology of the areas reviewed will be addressed in the Observations and Recommendations section of this report. Our examination would not reveal all weaknesses because it was based on selective review of data.

The internal control rating for each area reviewed is on page 4. These ratings quantify our opinion regarding the internal controls used in managing the systems and identify areas requiring corrective action.

It is our opinion that the overall internal control structure for the information systems at the Youth Center is weak. There were some specific problems noted that indicate the internal control structure could be more effective. Examples of the problems include the following.

- Youth does not have documented policies and procedures to address general controls over information systems. This may lead to inconsistent processes, system malfunction or failure, or compromised data.
- There is not a documented disaster and recovery plan to detail the exact steps to follow in the event of a major hardware or software failure.
- There is little or no monitoring of end-user processing, to include who is accessing a system and what actions are being taken. This may allow for unauthorized access or inappropriate system/data changes to go undetected.
- Documentation of vendor warranty and support for one system was missing or outdated.

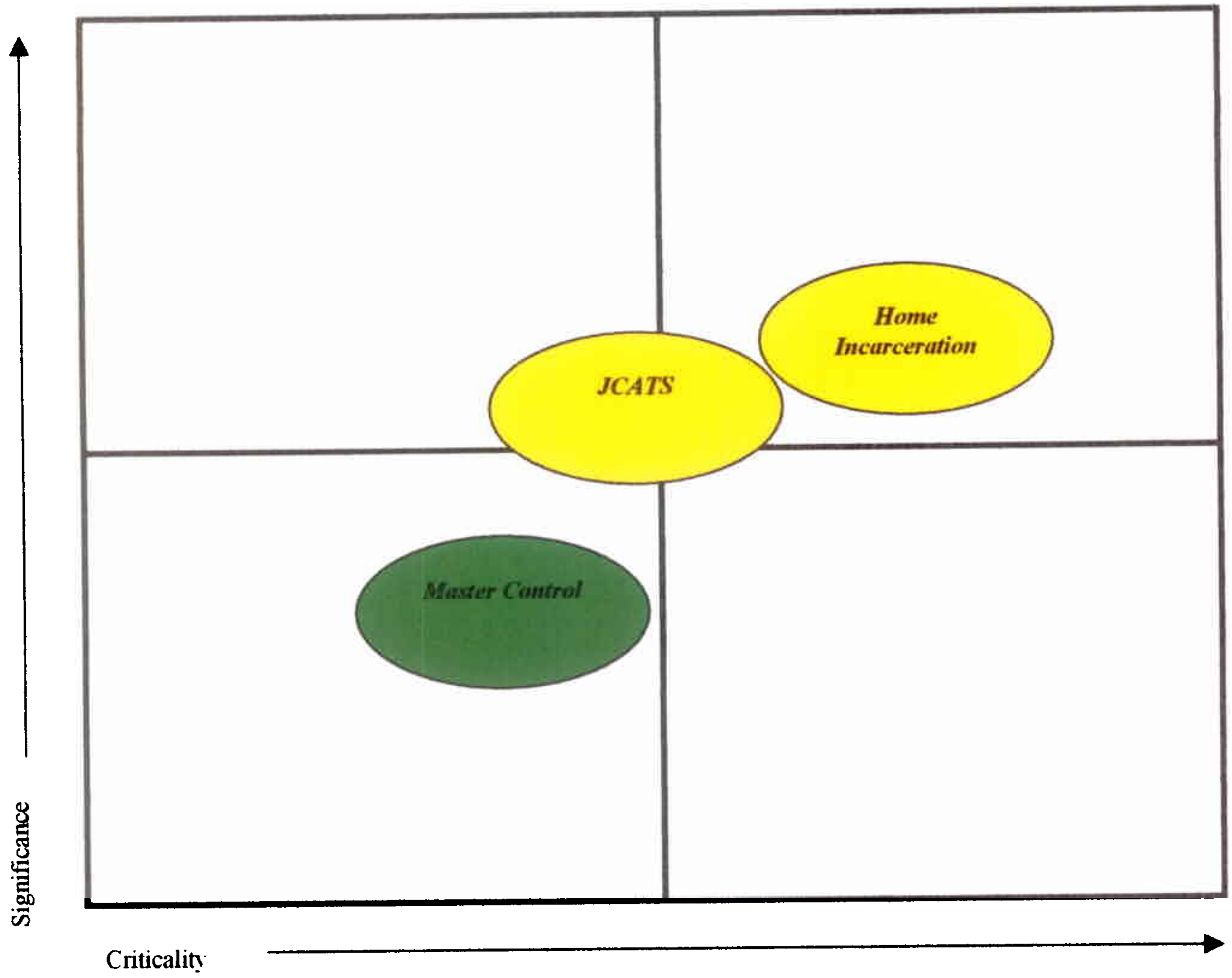
The implementation of the recommendations in this report will help improve the internal control structure and effectiveness of the Youth Center's information systems.

Michael S Norman

Michael S. Norman, CIA
Chief Audit Executive

cc: Louisville Metro Council Audit Committee
Louisville Metro Council Members
Deputy Mayors
Secretary of the Cabinet for Public Protection
Director of Youth Center
Director of Metro Technology

Internal Control Rating



Legend

Criteria	Satisfactory	Weak	Inadequate
Issues	Not likely to impact operations.	Impact on operations likely contained.	Impact on operations likely widespread or compounding.
Controls	Effective.	Opportunity exists to improve effectiveness.	Do not exist or are not reliable.
Policy Compliance	Non-compliance issues are minor.	Non-compliance issues may be systemic.	Non-compliance issues are pervasive, significant, or have severe consequences.
Image	No, or low, level of risk.	Potential for damage.	Severe risk of damage.
Corrective Action	May be necessary.	Prompt.	Immediate.

Introduction

The Youth Center operates per KRS 67.0831, which requires the local government to provide for a suitable facility or facilities for the custody and care of children held in custody pending disposition of their case by District and Circuit Courts. The facility is licensed to operate by the Kentucky Department of Juvenile Justice per KRS 15A and has maintained National Accreditation through the American Correctional Association since 1983. It is designed to ensure that all juveniles detained are housed in a safe and secure environment, which provides services that support juveniles' well-being through physical, mental, and social development.

Two major program units are essential for successful operation of the Youth Center, admissions and secure detention. Admissions provides processing and placement of every youth that is in custody. It tracks movement of all youth within the continuum and compiles statistical reports and other pertinent information. Secure Detention is the most secure and restrictive environment of local detention care that the courts can place juveniles (12-18 years of age) pending disposition of their case. This population of juveniles is charged with felonies, violent offenses, bench warrants, or they pose a serious threat to themselves or the community. The facility holds twelve living units with a ninety-six bed capacity.

The information systems used by the Youth Center are vital to their daily operations. These systems include the following.

- Home Incarceration System - The system used in daily operations to monitor and track youth assigned to the home incarceration program. It is an essential system in that it provides assurance that juveniles are adhering to court ordered actions.
- Juvenile Court Activity Tracking System (JCATS) - The database used to track all detained juveniles. This system provides Youth with a computerized inventory of all juveniles and corresponding pertinent information. It is used to track juveniles from the point of admission to their release date.
- Master Control Security System - The system is used to monitor and control security at the Youth Center. Specifically, it controls the electronic door locks and security cameras throughout the facility. This is a vital system to Youth in that they detain juveniles who are often charged with violent crimes and may pose a threat to themselves, as well as the community.

The fiscal year 2004 budget for the Youth Center is $6,473,800 for operating and $164,600 for capital. Specific capital expenditures are $119,000 for safety and security equipment and $45,600 for computer hardware.

This was a scheduled audit.

Summary of Audit Results

I. ***Current Audit Results***

See Observations and Recommendations section of this report.

II. *Prior Audit Issues*

The Office of Internal Audit has not previously audited the Youth Center's Information Systems General Controls.

III. *Statement of Auditing Standards*

Our audit was performed in accordance with Government Auditing Standards issued by the Comptroller General of the United States and with the Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors.

IV. *Statement of Internal Control*

We conducted a formal study of the internal control structure in order to obtain a sufficient understanding to support our final opinion.

V. *Statement of Irregularities, Illegal Acts, and Other Noncompliance*

Our examination did not disclose any instances of irregularities, any indications of illegal acts, and nothing came to our attention during the examination that would indicate evidence of such. Any significant instances of noncompliance with laws and regulations are reported in the Observations and Recommendations section of this report.

VI. *Views of Responsible Officials*

An exit conference was held at the Youth Center administrative office on March 22, 2004. Attending were Clarence Williams, Sandra Wilson, Pat Nurse and Elton Jackson representing the Youth Center; Mike Norman and Mary Ann Wheatley representing Internal Audit. Final audit results were discussed.

The views of the Youth Center officials are included as responses in the Observations and Recommendations section of the report.

Observations and Recommendations

Home Incarceration

Scope

Interviews were held with key personnel from Youth Center in order to obtain an understanding of their Home Incarceration system. This system is used in daily operations to monitor and track youth assigned to home incarceration. The system stores an inventory of equipment (anklets and boxes), as well as information regarding each juvenile assigned to the program. Each juvenile is linked to specific equipment. The anklet is placed on the juvenile's ankle and the box is connected to a telephone outlet at the juvenile's home. Monitoring of the juvenile's activity is possible via communication between the box and main system/server. The box communicates any deviations from the youth's assignment (e.g. anklet removed) to the main system, which in turn pages the juvenile's Senior Social Worker. All assignment violations and equipment malfunctions are registered on the system's hard drive.

The current system equipment and software was leased from an outside vendor – BI, Inc – beginning in 1999. The vendor provides system support and maintenance. All system components, to include the computer, monitor, server, and such are housed at Youth.

The adequacy of the general controls governing the system were reviewed to ensure assets are adequately safeguarded, data files and software are secured, technical and administrative support are adequate, and management support and awareness of the system function are adequate. Policy documents, security measures, and such may have been reviewed for proof of existence, but in-depth technical system testing was not performed.

Observation #1 – General Operations

There were some control weaknesses noted with the general operations of the Youth Center's Home Incarceration system. Specific examples include the following.

- Youth does not have documented policies and procedures to address information systems general controls. Youth is currently following a somewhat dated policy and procedures manual that was developed when they were a division of the Department of Human Services, prior to merger of Metro Government. This manual addresses some areas that might also be included in an information systems manual but not in sufficient detail.

- It could not be verified with certainty if the Home Incarceration system is currently under warranty and support from the vendor.

- ➢ Youth personnel provided a vendor Software License, Warranty and Support document for the Home Incarceration system but it was not signed and appeared to be outdated (December 20, 2000). A letter from the vendor, dated March 15, 2001, was also provided and stated that an "extended Warranty Agreement is in the process of signature". However, Youth could not provide a signed version of this document.
- ➢ Hardware for the Home Incarceration program was leased from a vendor for the past few years. Included in the lease payment was a maintenance fee that ensured vendor support. However, per an amortization schedule of lease payments, Youth's final lease payment was due December 2003. Though Youth has the option to buy the equipment and to purchase continued support from the vendor, Youth personnel could not verify if these purchases had been made.

- Though it was stated that the Home Incarceration system is rarely down, Youth personnel do not maintain a log of system downtime/device errors or a log of vendor support servicing. This makes it difficult to monitor if the system is functioning at an acceptable level to support Youth's needs.

- There is not a current listing of all system hardware/software for the Home Incarceration system and components have not been given an asset number or identification mark to assist in accountability of inventory. It should be noted that Youth is currently working on a department asset listing.

Recommendations

Appropriate Youth Center personnel should take corrective action to address the general operating concerns noted with the Home Incarceration system.

✓ A policy and procedures manual should be developed and documented to reflect the current practices of the Youth Center. A section regarding information systems should be incorporated to provide guidelines as to safeguarding equipment, authorized users, system maintenance, continuity of operations during system down times, equipment purchase procedures, system change control and other related activities. The manual helps promote uniformity across an organization and should be distributed to all Youth personnel.

✓ Appropriate Youth personnel should determine if Home Incarceration computer equipment should be/or has been purchased from the vendor. In addition, any warranty and support agreements or maintenance agreements should be reviewed to determine if they are current and valid documents. Copies of any future agreements entered into with the vendor should be obtained and kept as support of agreement terms. System warranty and support, as well as maintenance, help ensure a system is functioning as intended.

✓ Youth personnel should maintain a log of system downtime or device errors. The log should also note any vendor support servicing the system receives. This would provide a documented record of system problems and help in the detection of recurring problems.

✓ Youth personnel stated they are currently working on an asset listing for their department. They should continue to develop this document and assign responsibility for upkeep to a specific individual. Though some computer equipment may not reach the threshold of a true asset listing, it would be beneficial to maintain this information on the listing or a separate listing. An inventory listing of all computer equipment is essential to effectively safeguard assets. The inventory list should include desktops, printers, servers, software, etc. and should contain a unique identification number or serial number for each item.

Observation #2 – Business Continuity

Some weaknesses were noted that could hinder Home Incarceration system processes from being recovered following a system failure or disaster. Specific examples include the following.

- There is not a documented disaster and recovery plan to detail the exact steps to follow in the event of a major hardware or software failure. Though manual processes can often be implemented in the event of a system failure, these processes do not address a true disaster that might require physical relocation.

- Current practices regarding database backups for the Home Incarceration system may not be adequate to ensure a proper recovery.

    - ➢ Though backups are performed daily, automatically by the system, there are only two discs used in the process. One is always in the server to record the next backup and the other holds the previous day's backup. This may not be a sufficient supply of backup discs in that if a system error went undetected for more than one day, Youth would not have a backup disc containing 'good' data.

    - ➢ The backup disc is stored on top of the server for use the next day. This practice would be ineffective in that if a disaster were to occur at the Youth Center, both the server and the backup disc could be destroyed.

- Though backups of system data are performed daily, it does not appear that the backup of the *server* is a function of Youth. The vendor should be contacted to ensure they perform such a backup on a regular basis.

- There were some weaknesses noted with regards to environmental controls over the Home Incarceration system.

    - ➢ Though the current server has not been exposed to any water leaks, it is located in an office only a few feet away from where a water leak ruined the prior server. Water pipes are located above the office ceiling. This may not be a good location to adequately safeguard the system components from future water damage.

- ➢ There is not a documented policy to prohibit the consumption of food and beverages within the server environment. Though the system is generally not exposed to these items, they pose risks to system components.

Recommendations

Youth personnel should take corrective action to address the weaknesses noted to ensure continuity of the Home Incarceration system.

- ✓ The Home Incarceration system is essential for the successful operation of the Youth Center. A disaster and recovery plan should be developed to document the processes to follow in the event of a true emergency. Ideally, backups of systems would be available at a remote location to allow business to continue if a disaster was to occur at the Youth Center. The plan should be specific as to exact procedures to follow, assign responsibility to individuals, and should be communicated to all appropriate personnel. The plan should be stored offsite and should be reviewed, tested, and updated routinely to ensure effectiveness. Youth should coordinate with the Metro Department of Technology to include their plan in the overall Metro Government disaster and recovery plan.

- ✓ More than one day's backup should be retained to provide an ample amount of backup information for a system (i.e. one weeks worth). This would help in the restoration of good data in a case where an error went undetected for more than a day. In addition, backup tapes/discs should be stored offsite to provide the most benefit in the event of a disaster at the location of the server.

- ✓ The vendor supporting the Home Incarceration system should be contacted to ensure system backups are being performed routinely. This is essential considering the reliance placed on the vendor to keep the system up and running.

- ✓ Youth should consider if there is a better location within its facility to house the Home Incarceration system, preferably a secure area where there are no water pipes in the ceiling above it.

- ✓ A consumption policy should be documented to help prevent system damage from exposure to food and beverages. This policy should apply to all computer systems, not just Home Incarceration, and should be clearly communicated to all personnel.

Observation #3 – Security

There were security weaknesses noted that could hinder the confidentiality, integrity and availability of information within the Home Incarceration system.

- There were some control weaknesses where the security of data files or transactions could be compromised or lost.

- ➢ End-user processing is not subject to an audit trail. Though Youth staff compares source documents (e.g. court orders) to the system to ensure data was entered appropriately, improper edits of data could possibly go undetected since change reports are not generated and monitored.
- ➢ Though there are limited functions performed by Youth personnel on the Home Incarceration server, no one at Youth monitors access and use of the server for appropriateness. Additionally, there is not an identifying or reporting mechanism in place to help in the detection of unauthorized users.
- ➢ The vendor dials-in to Youth's Home Incarceration system frequently to ensure the system and equipment are functioning properly. There are risks associated with using a modem and it is essential to ensure that proper safeguards are in place to reduce these risks.
- ➢ Though system users enter a unique logon ID when accessing the system, the password for the system is shared among all users. It is not a policy to have the password changed periodically or to have the system force changes.
- ➢ Logon sessions do not automatically logoff after a short period of inactivity. Also, logons are not deactivated after no use for a specified period of time. Both of these practices could allow for unauthorized users to more easily access the system.

- There is no standard form to complete to add/delete/change access to the Home Incarceration system. Though additions are only made on a need-to-know basis, based on job function, the process for additions/deletions and signature authorizations is not documented.

- A hard copy user manual is stored next to the Home Incarceration computer. However, agency policy and procedure states that the manual is to be kept confidential and "locked in a desk/file cabinet. Under no circumstances should the Instruction Book lie about the office." Leaving a systems manual unsecured increases the risk of unauthorized access.

- Metro Department of Technology installs virus detection software on all Metro computers. However, Youth was not certain if the Home Incarceration computer had the virus detection software installed on it. The equipment was leased but just recently Youth may have acquired ownership.

Recommendations

Appropriate Youth personnel should take corrective action to ensure system information is properly safeguarded.

- ✓ Measures should be taken to ensure information system data is secured from unauthorized access, unauthorized changes, and loss. Reports of data changes should be generated and monitored for appropriateness. Items to be reviewed for appropriateness include who is accessing the system, what are they accessing, what changes are they making, and such, to ensure integrity of data.

✓ Appropriate Youth personnel should contact the vendor to ensure adequate measures have been taken on their part to safeguard the Home Incarceration system. Specifically, Youth should inquire about the vendor's security measures for the dial-up function and backup processes for the system server. If Youth does not feel they have the technical expertise to make a determination as to whether measures are adequate, they should contact Metro Department of Technology for their assistance/opinion.

✓ A password policy should be developed to help ensure data is safeguarded from unauthorized access. Users should create their own unique password and keep it confidential. The policy should prohibit popular or easy to guess passwords and should set parameter requirements (i.e. at least 7-14 characters in length, a mix of alpha and numeric characters, no re-use, disable workstation after 3 unsuccessful attempts, etc.). In addition, a current encryption algorithm should be used to help prevent hacking of passwords.

✓ User logon sessions should automatically logoff after a short period of inactivity and should be deactivated after no use for a specified period of time. Both of these practices could help prevent unauthorized users from accessing the system.

✓ Youth should create a standard form to be used when adding/deleting/changing a user's access rights to a system. Supervisory signature authorization should be noted on the form to indicate approval of the request. Use of the form should be addressed in a policy manual to ensure consistency throughout the department. Also, it should specifically address the deletion of users from a system upon transfer or termination.

✓ System user manuals should be securely stored and kept confidential according to policy requirements.

✓ It is essential that virus detection software be installed on all computers to help protect data files. Youth should contact the vendor to inquire if this software has been installed or what steps are necessary to get it installed.

Youth Center's Response

Youth Center personnel have reviewed the Information Systems General Controls Audit Report. The department is in concurrence with the recommendations of the report, and they intend to address the findings within their control. Specific actions to be taken include the following.

- Update and document policies and procedures to address general controls over information systems.
- Obtain documentation of all current agreements with vendors regarding system warranty and support.
- Maintain logs of system downtime and vendor support servicing.

Some recommendations require actions from vendors and other Metro departments besides the Youth Center. Youth personnel intend to make it a priority to work with these entities to ensure all findings are addressed.

Juvenile Court Activity Tracking System (JCATS)

Scope

Interviews were held with key personnel from Youth Center in order to obtain an understanding of the database used to track detained youth – Juvenile Court Activity Tracking System (JCATS). Information recorded in the database includes admissions (intake/release), court appointments, warrants, visitation, charges, assignment area, and much more. The JCATS database was purchased from an outside vendor - Canyon Solutions. Youth enters into a yearly lease agreement with Canyon Solutions, which entitles them to one site license (installation on one server) and unlimited user licenses (concurrent access to the system via multiple workstations). Canyon Solutions performs modifications to the JCATS database as needed/upon request by Youth.

Note: The server that holds the JCATS software is housed at the Department of Human Services (DHS) and supported by their technology personnel. Youth was a division of DHS prior to merger of Louisville Metro Government (January 2003). Currently, Youth, DHS and Metro Department of Technology personnel are working with Canyon Solutions to develop JCATS as a web-based system. It is planned that this version will go live within the next couple of months. The server housed at DHS will no longer be used when the web-based version is implemented. Rather, the new server will be housed and maintained by Metro Department of Technology personnel.

The adequacy of the general controls governing the system were reviewed to ensure assets are adequately safeguarded, data files and software are secured, technical and administrative support are adequate, and management support and awareness of the system function are adequate. Policy documents, security measures, and such may have been reviewed for proof of existence, but in-depth technical system testing was not performed.

Observation #1 – General Operations

There were some control weaknesses noted with the general operations of Youth Center's JCATS. Specific examples include the following.

- Youth does not have documented policies and procedures to address information systems general controls, to include proper database administration (i.e. segregation of duties, access authority). Youth is currently following a somewhat dated policy and procedures manual that was developed when they were a division of the Department of Human Services, prior to merger of Metro Government. This manual addresses some areas that might also be included in an information systems manual but not in sufficient detail.

- A JCATS user manual exists but is very old and outdated. Therefore it is not used as a training tool for end-users.

- There were some weaknesses noted with regards to JCATS hardware and software inventory management. These weaknesses make safeguarding and accountability of inventory difficult to ensure.
  - ➢ Youth does not maintain a current listing of all system hardware and software for JCATS.
  - ➢ System components have not been given an asset number or identification mark to assist in accountability of inventory.
  - ➢ There is not a documented policy regarding the disposal of obsolete computer equipment.

- Youth personnel do not maintain a log of system downtime/device errors or a log of vendor support servicing. This makes it difficult to monitor if the system is functioning at an acceptable level to support Youth's needs.

- The Management Analyst assigned the responsibility of managing the JCATS system may need additional technical training due to the job functions and responsibilities assigned to the position.

Recommendations

Youth personnel should take corrective measures to help ensure the general operating processes and procedures for JCATS are efficient and effective to allow the system to function as intended. Specific recommendations include the following.

✓ A policy and procedures manual should be developed and documented to reflect the current practices of the Youth Center. A section regarding information systems should be incorporated to provide guidelines as to safeguarding equipment, authorized users, system maintenance, continuity of operations during system down times, equipment purchase procedures, system change control, database administration and other related activities. The manual helps promote uniformity across an organization and should be distributed to all Youth personnel.

✓ An updated user manual should be developed to reflect the current processes and procedures to follow when using the system. The manual, and any subsequent updates to it, should be distributed to all personnel that use the system. It should be used as part of the training process for new employees, as well as a reference tool for others.

✓ Youth personnel stated they are currently working on an asset listing for their department. They should continue to develop this document and assign responsibility for upkeep to a specific individual. Though some computer equipment may not reach the threshold of a true asset listing, it would be beneficial to maintain this information on the listing or a separate listing. An inventory listing of all computer equipment is essential to effectively safeguard assets. The inventory list should include desktops, printers, servers, software, etc. and should contain a unique identification number or serial number for each item. There should also be a documented policy in place to address the disposal of any obsolete equipment.

- ✓ Youth personnel should maintain a log of JCATS downtime or device errors. The log should also note any vendor support servicing the system receives. This would provide a documented record of system problems and help in the detection of recurring problems. This log should be used as a monitoring tool to determine if the system is functioning at an acceptable level to provide the Youth Center with adequate information.

- ✓ Once the JCATS system upgrade is made, additional training needs of Youth personnel should be accessed based on new job functions and responsibilities.

Observation #2 – Business Continuity

There is not a documented disaster and recovery plan to detail the exact steps to follow in the event of a major hardware or software failure. Though manual processes can often be implemented in the event of a system failure, these processes do not address a true disaster that might require physical relocation.

Recommendations

JCATS is essential for the successful operation of the Youth Center. A disaster and recovery plan should be developed to document the processes to follow in the event of a true emergency. Ideally, backups of systems would be available at a remote location to allow business to continue if a disaster were to hit the Youth Center. The plan should be specific as to exact procedures to follow, assign responsibility to individuals, and should be communicated to all appropriate personnel. The plan should be stored offsite and should be reviewed, tested, and updated routinely to ensure effectiveness. Youth should coordinate with the Metro Department of Technology to include their plan in the overall Metro Government disaster and recovery plan.

Observation #3 – Security

There were security weaknesses noted that could hinder the confidentiality, integrity and availability of information within JCATS. Specifics include the following.

- There were some control weaknesses where the security of data files or transactions could be compromised or lost.
  - ➢ Access to the database and capabilities within it are based on the access group an employee is assigned to. Anyone can make changes to data if they can access the application panel. Changes to data (excluding addition/deletion of records) cannot be directly traced to an individual.

- ➢ There is not an identifying or reporting mechanism in place to help in the detection of unauthorized users or data changes. Monitoring of data changes is not performed.
- ➢ The vendor has remote access to the JCATS system in order to assist when the system malfunctions or there might be an error with a particular record. Though it can be very beneficial for the vendor to have system access when troubleshooting, there are inherent risks with remote access that lessen data security.
- ➢ System passwords are issued to end-users by the Management Analyst. They are not required to be changed periodically and the system does not force changes. There may be cases where users are still using their original password.
- ➢ End-users are not completely deleted from the system upon transfer or termination. Their password is changed but their logon ID is not removed.
- ➢ The encryption algorithm to protect passwords is approximately four years old. An algorithm this old is usually easily hackable.
- ➢ Logon sessions do not automatically logoff after a short period of inactivity. Also, logon IDs are not deactivated after no use for a specified period of time.

- There is no standard form to complete to add/delete/change access to the JCATS system. Though additions are only made on a need-to-know basis, based on job function, the process for additions/deletions and signature authorizations is not documented.

Recommendations

Appropriate Youth personnel should take corrective action to help ensure security measures are adequate to safeguard information in JCATS.

✓ Measures should be taken by appropriate personnel to ensure information system data is secured from unauthorized access, unauthorized changes, and loss. Reports of data changes should be generated and monitored for appropriateness. Items to be reviewed for appropriateness should include who is accessing the system, what are they accessing, what changes are they making, and such, to ensure data integrity. It may be necessary to contact the supporting vendor to inquire about necessary reports and tracking of transactions.

✓ Appropriate Youth personnel should contact the vendor to ensure adequate measures have been taken on their part to safeguard JCATS. Specifically, Youth should inquire about the vendor's security measures for their remote access. If Youth does not feel they have the technical expertise to make a determination as to whether measures are adequate, they should contact Metro Technology for their assistance/opinion.

✓ A password policy should be developed to help ensure data is safeguarded from unauthorized access. Users should create their own unique password and keep it confidential. The policy should prohibit popular or easy to guess passwords and should set parameter requirements (i.e. at least 7-14 characters in length, a mix of alpha and numeric characters, no re-use, disable workstation after three unsuccessful attempts, etc.). In addition, a current encryption algorithm should be used to help prevent hacking of passwords.

- ✓ User logon sessions should automatically logoff after a short period of inactivity and should be deactivated after no use for a specified period of time. Both of these practices could help prevent unauthorized users from accessing the system.
- ✓ Youth should create a standard form to be used when adding/deleting/changing a user's access rights to a system. Supervisory signature authorization should be noted on the form to indicate approval of the request. Use of the form should be addressed in a policy manual to ensure consistency throughout the department. Also, it should specifically address the deletion of users from a system upon transfer or termination.

Observation #4 – Server Support

The JCATS server is house at the Department for Human Services and is supported by their technology staff. An upgraded version of the system is currently being developed by an outside vendor, Youth Center, Human Services and Metro Department of Technology (DOT) personnel. It is intended that when the new version is ready for implementation, the server will then be housed and supported by Metro DOT. The following concerns were noted with the current server being housed and supported by Human Services.

- Though processes are understood through experience and training, server operating procedures, to include the recovery of databases during interruption of services, are not documented.
- Server backup procedures may not be sufficient to ensure the most up-to-date information is available during a system failure.
  - ➢ Though DHS staff performs server backups nightly during the week (Mon.-Fri.), the Youth Center is operational seven days a week. Therefore, data entered on the weekend is at risk for being lost since it is not backed up until Monday evening.
  - ➢ Though backup tapes are stored in a locked room, the room is located down the hall from the server facility. This may not be an adequate distance from the server should a true disaster occur.
- Server utilization is not routinely monitored to ensure only authorized personnel are accessing the system. Instead, a performance monitoring tool is usually only run as problems occur.
- It was stated that disk storage space is frequently a problem so it is monitored closely and data is often archived.

- There were some physical and environmental weaknesses noted with regards to the server facility that could compromise the well being of system components by increasing the risk of theft, physical damage and such.
  - ➢ The server facility may not be reasonably protected from forced entry. There is a glass window in the door that could be broken and allow for easy access to the server room.
  - ➢ There are no fire protection devices within the server room (e.g. fire extinguisher, smoke detector).
  - ➢ There is evidence of water leaks in the ceiling, and it was stated that measures had to be taken in the past to protect the server from water damage (plastic coverings were placed over the server).
  - ➢ No smoking, food, or open container drink is allowed in the server room but this policy is not documented.
  - ➢ Though the server facility appeared clean, there is not a documented cleaning schedule to ensure system components are routinely maintained.

Recommendations

Since the JCATS database is being upgraded to a more sophisticated version and the server will be housed under the direct support of Metro Department of Technology (DOT), many control weaknesses noted may be rectified with little or no additional actions by Youth or Human Services personnel. However, since Youth is the owner of the system, appropriate personnel should follow-up with Metro DOT personnel and become familiar with their processes to ensure all weaknesses are addressed (i.e. secure and clean environment, adequate backup procedures, limited access to server facility, etc.).

Youth Center's Response

See response in Home Incarceration section of this report.

Master Control

Scope

Interviews were held with key personnel from Youth Center in order to obtain an understanding of their security system known as Master Control. The system is used to monitor and control security at the facility. Specifically, it controls the electronic door locks and security cameras throughout the facility. The system was purchased from and is supported by an outside vendor (integrator.com). All system components, to include the computer, monitor, server, and such are housed at Youth.

The adequacy of the general controls governing the system were reviewed to ensure assets are adequately safeguarded, data files and software are secured, technical and administrative support are adequate, and management support and awareness of the system function are adequate. Policy documents, security measures, and such may have been reviewed for proof of existence, but in-depth technical system testing was not performed.

Observation #1 – General Operations

Though the overall general operations of the Youth Center's Master Control system were satisfactory, there were a few control weaknesses noted. However, these are not likely to impact Youth's operations since manual processes can be implemented in place of the computer system. Specific examples include the following.

- Youth does not have documented policies and procedures to address information systems general controls. Youth is currently following a somewhat dated policy and procedures manual that was developed when they were a division of the Department of Human Services, prior to merger of Metro Government. This manual addresses some areas that might also be included in an information systems manual but not in sufficient detail.

- Youth was operating under an expired service contract for the Master Control system. A service agreement renewal document provided from the vendor, dated November 10, 2003, noted that the Youth Center's current service contract had expired October 14, 2003. The renewal document had not been signed to signify agreement to terms and continued coverage for another year.

- There were some weaknesses noted with regards to the security system's hardware and software inventory management.
    - ➢ Youth does not maintain a current listing of all system hardware and software for Master Control.
    - ➢ System components have not been given an asset number or identification mark to assist in accountability of inventory.

- ➢ There is not a documented policy regarding the disposal of obsolete computer equipment.

- Youth personnel do not maintain a log of system downtime/device errors or a log of vendor support servicing. This makes it difficult to monitor if the system is functioning at an acceptable level to support Youth's needs.

Recommendations

Youth personnel should take corrective measures to help ensure the general operations for the Master Control system are adequate to allow the system to function as intended.

- ✓ A policy and procedures manual should be developed and documented to reflect the current practices of the Youth Center. A section regarding information systems should be incorporated to provide guidelines as to safeguarding equipment, authorized users, system maintenance, continuity of operations during system down times, equipment purchase procedures, system change control and other related activities. The manual helps promote uniformity across an organization and should be distributed to all Youth personnel.

- ✓ Appropriate Youth personnel should determine if continued vendor support servicing is warranted for the Master Control system. If so, the renewal agreement should be signed to indicate agreement to contract terms and forwarded to the vendor so coverage can begin immediately. Vendor support servicing helps ensure a system is functioning as intended. Agreements should be monitored closely to help prevent the expiration of desired services.

- ✓ Youth personnel stated they are currently working on an asset listing for their department. They should continue to develop this document and assign responsibility for upkeep to a specific individual. Though some computer equipment may not reach the threshold of a true asset listing, it would be beneficial to maintain this information on the listing or a separate listing. An inventory listing of all computer equipment is essential to effectively safeguard assets. The inventory list should include desktops, printers, servers, software, etc. and should contain a unique identification number or serial number for each item. There should also be a documented policy in place to address the disposal of any obsolete equipment.

- ✓ Youth personnel should maintain a log of Master Control system downtime or device errors. The log should also note any vendor support servicing the system receives. This would provide a documented record of system problems and help in the detection of recurring problems. This log should be used as a monitoring tool to determine if the system is functioning at an acceptable level to provide the Youth Center, as well the community, with adequate security.

Observation #2 – Business Continuity

Though the Youth Center does not have a documented disaster and recovery plan to detail the exact steps to follow in the event of a major hardware or software failure, manual processes can be implemented to ensure facility security. However, these processes do not address a true disaster that might require physical relocation.

Recommendations

The Master Control system is essential for the successful operation of the Youth Center. A disaster and recovery plan should be developed to document the processes to follow in the event of a true emergency. The plan should be specific as to exact procedures to follow, assign responsibility to individuals, and should be communicated to all appropriate personnel. The plan should be stored offsite and should be reviewed, tested, and updated routinely to ensure effectiveness.

Youth Center's Response

See response in Home Incarceration section of this report.